



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/754,813	01/04/2001	Jing Min Xu	JP919990266US1	3476

7590

01/02/2004

Ido Tuchman
69-60 108th Street
Suite 503
Forest Hills, NY 11375

EXAMINER

CHEN, CHONGSHAN

ART UNIT

PAPER NUMBER

2172

DATE MAILED: 01/02/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/754,813

Applicant(s)

XU ET AL.

Examiner

Chongshan Chen

Art Unit

2172

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 13 November 2003.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-20 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-20 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. §§ 119 and 120

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
* See the attached detailed Office action for a list of the certified copies not received.
- 13) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.
a) ☐ The translation of the foreign language provisional application has been received.
- 14) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____
- 4) ☐ Interview Summary (PTO-413) Paper No(s). _____
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____

Art Unit: 2172

DETAILED ACTION

1. This action is responsive to communications: RCE, filed on 11/13/2003. This action is non-final. Claims 1-15 and 17-21 are pending. There is no claim 16 in the claim.

Claim Rejections - 35 USC § 112

2. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claims 10 and 13 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

4. The terms "black list" in claim 10 and "black lists" in claim 13 are not defined in the specification.

Claim Objections

5. Claims 1, 5, 11 and 18 are objected to because of the following informalities: please spell out the terms "API" and "RFC1424" in the claims. Appropriate correction is required.

Response to Arguments

6. Applicant's arguments filed on 11/13/03 regarding claim 1, Kocher does not disclose a CRL access user interface for providing a uniform set of APIs for users accessing the CRLs in the CRL database, said system enabling consolidation and access of the certificate revocation lists (CRLs) from the plurality of certificate authorities (CAs), have been fully considered.

Art Unit: 2172

Kocher teaches the system enabling consolidation and access of the certificate revocation lists (CRLs) (Kocher, col. 3, lines 15-18). Kocher does not explicitly disclose a CRL access user interface for providing a uniform set of APIs for users accessing the CRLs in the CRL database. Ng (6,411,956) teaches an access user interface for providing a uniform set of APIs for users accessing the database (Ng, col. 1, lines 15-18). APIs can access database with all kinds of data stored in the database. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to provide a uniform set of APIs for users accessing the CRLs in the system of Kocher. This provides an easy access to the CRLs using a single uniformed interface instead of using different interfaces for each different CRL.

7. In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., creating a plurality of CRL retrieval agents based on the CRL distribution mechanisms of CAs) are not recited in the rejected claim 1. Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

8. As per applicant's arguments regarding claim 1, "Kocher does not teach or suggest retrieval agents based on the CRL distribution " have been considered but are not persuasive. An agent is a switch or switch-like component or bridge between the requester and the responder (IEEE 100: The Authoritative Dictionary of IEEE Standards Terms). A system requests to verify whether a digital signature is valid. The CRLs responds the request and accesses the CRLs to determine whether the certificate in question is revoked. If the certificate is not on the list, it is assumed to be valid. Clearly, there are agents/bridges which connect the requesters which

Art Unit: 2172

request the status of certificates with the responders/CRLs/CAs in order to verify whether the certificates are valid.

9. As per applicant's arguments regarding claim 11 and 18, "creating a plurality of CRL retrieval agents based on the CRL distribution mechanisms of CAs, for consolidating the CRLs from multiple CAs" have been considered but are not persuasive. Kocher teaches consolidating the CRLs from multiple CAs (Kocher, col. 3, lines 15-18, "allow revocations from many CAs to be included efficiently in a single database ..."). Furthermore, an agent is a switch or switch-like component or bridge between the requester and the responder (IEEE 100: The Authoritative Dictionary of IEEE Standards Terms). A system requests to verify whether a digital signature is valid. The CRLs responds the request and accesses the CRLs to determine whether the certificate in question is revoked. If the certificate is not on the list, it is assumed to be valid. Clearly, there are plurality of agents/bridges which connect the requesters which request the status of certificates with their corresponding responders/CRLs/CAs in order to verify whether the certificates are valid.

Claim Rejections - 35 USC § 103

10. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

11. Claims 1-2, 4, 6-8, 10-15, and 17-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kocher (6,442,689) in view of Ng (6,411,956).

As per claim 1, Kocher teaches a system comprising:

a plurality of certificate authorities (CAs) in which each CA maintains and distributes digital certificates revoked by itself in the form of a certificate revocation list (CRL), and different CAs may use different CRL distribution mechanisms (Kocher, Abstract, col. 2, lines 17-31, col. 3, lines 15-18);

a plurality of CRL databases for storing the consolidated CRLs from multiple CRL retrieval agents and/or the replications of CRLs, the CRL databases storing at least one individually identifiable revoked digital certificate (Kocher, Abstract, col. 3, lines 15-18).

Kocher does not explicitly disclose a CRL access user interface for providing a uniform set of APIs for users accessing the CRLs in the CRL database. Ng teaches an access user interface for providing a uniform set of APIs for users accessing the database (Ng, col. 1, lines 15-18). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to provide a uniform set of APIs for users accessing the CRLs in the system of Kocher. This provides an easy access to the CRLs using a single uniformed interface instead of using different interfaces for each different CRL.

As per claim 2, Kocher and Ng teach all the claimed subject matters as discussed in claim 1, and further disclose said plurality of CRL databases include a central CRL database and a plurality of CRL replication databases, said central CRL database for storing the consolidated CRLs from the multiple CRT, retrieval agents, and said plurality of CRL replication databases for storing the replications of the CRLs of the central CRL database (Kocher, Abstract, col. 2, lines 17-31, col. 3, lines 15-18).

As per claim 4, Kocher and Ng teach all the claimed subject matters as discussed in claim 1, and further disclose said plurality of CRL retrieval agents include a HTTP/CRL retrieval agent, for periodically retrieving CRLs from specified HTTP servers and updating the CRL database (Kocher, col. 1, line 19 - col. 2, line 67).

As per claim 6, Kocher and Ng teach all the claimed subject matters as discussed in claim 1, and further disclose said plurality of CRL retrieval agents include a HTTP retrieval agent triggered by a HTTP request, said HTTP receiver agent verifies an authorization of the requester, if successful, said agent stores each transmitted CRL in the CRL databases (Kocher, col. 3, line 1 - col. 4, line 56, col. 10, lines 64-67).

As per claim 7, Kocher and Ng teach all the claimed subject matters as discussed in claim 1, and further disclose said plurality of CRL retrieval agents further verifies the integrity and the authenticity of the retrieved CRLs (Kocher, col. 3, line 1 - col. 4, line 56).

As per claim 8, Kocher and Ng teach all the claimed subject matters as discussed in claim 1, and further disclose a particular replication architecture is used among said plurality of CRL databases in order to maintain database consistency (Kocher, col. 2, line 17 - col. 4, line 57).

As per claim 10, Kocher and Ng teach all the claimed subject matters as discussed in claim 1, and further disclose said system is also adapted for consolidating and accessing at least one kind of black list (Kocher, col. 3, line 1 - col. 4, line 56).

As per claim 11, Kocher teaches in a secure network implemented by digital certificates, a method for certificate revocation list (CRL) consolidation and access, wherein a plurality of certificate authorities (CAs) maintain and distribute the digital certificates revoked by themselves

Art Unit: 2172

in the form of CRLs, and different CAs may use different CRL distribution mechanisms, said method comprising the steps of:

creating a plurality of CRL retrieval agents based on the CRL distribution mechanisms of CAs, for consolidating the CRLs from multiple CAs (Kocher, Abstract, col. 2, line 17 - col. 3, line 18);

storing the consolidated CRLs from multiple CRL retrieval agents or the replications of CRLs into a plurality of CRL databases, the consolidated CRLs including at least one individually identifiable revoked digital certificate (Kocher, Abstract, col. 2, line 17 - col. 3, line 18).

Kocher does not explicitly disclose accessing the CRLs from the CRL databases by a uniform set of APIs. Ng teaches an access user interface for providing a uniform set of APIs for users accessing the database (Ng, col. 1, lines 15-18). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to provide a uniform set of APIs for users accessing the CRLs in the system of Kocher. This provides an easy access to the CRLs using a single uniformed interface instead of using different interfaces for each different CRL.

Claim 12 is rejected on grounds corresponding to the reasons given above for claim 2.

As per claim 13, Kocher and Ng teach all the claimed subject matters as discussed in claim 11, and further disclose said method is also adapted for consolidation and accessing all kinds of black lists (Kocher, col. 3, line 1 - col. 4, line 56).

As per claim 14, Kocher and Ng teach all the claimed subject matters as discussed in claim 11, and further disclose an article of manufacture comprising a computer usable medium

Art Unit: 2172

having computer readable program code means embodied therein for causing certificate revocation list (CRL) consolidation and access, the computer readable program code means in said article of manufacture comprising computer readable program code means for causing a computer to effect the steps of claim 11 (Kocher, col. 1, line 1 - col. 4, line 56).

As per claim 15, Kocher and Ng teach all the claimed subject matters as discussed in claim 11, and further disclose a computer program product comprising a computer usable medium having computer readable program code means embodied therein for causing certificate revocation list (CRL) consolidation and access, the computer readable program code means in said computer program product comprising computer readable program code means for causing a computer to effect the steps of claim 11 (Kocher, col. 1, line 1 - col. 4, line 56).

As per claim 17, Kocher and Ng teach all the claimed subject matters as discussed in claim 11, and further disclose a program storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform method steps for certificate revocation list (CRL) consolidation and access, said method steps comprising the steps of claim 11 (Kocher, col. 1, line 1 - col. 4, line 56).

Claim 18 is rejected on grounds corresponding to the reasons given above for claim 11.

Claim 19 is rejected on grounds corresponding to the reasons given above for claim 17.

Claim 20 is rejected on grounds corresponding to the reasons given above for claim 14.

Claim 21 is rejected on grounds corresponding to the reasons given above for claim 15.

12. Claim 3 is rejected under 35 U.S.C. 103(a) as being unpatentable over Kocher (6,442,689) in view of Ng (6,411,956) and further in view of Vesna Hassler ("Hassler", "X.500

Art Unit: 2172

and LDAP security: a comparative overview”, Network, IEEE, Volume: 13 Issue: 6, Nov.-Dec. 1999, Page(s): 54-64).

As per claim 3, Kocher and Ng teach all the claimed subject matters as discussed in claim 1, except for explicitly disclosing said plurality of CRL retrieval agents include a LDAP/CRL retrieval agent, for periodically retrieving CRLs from specified LDAP servers and updating the CRL databases. Hassler discloses said plurality of CRL retrieval agents include a LDAP/CRL retrieval agent, for periodically retrieving CRLs from specified LDAP servers and updating the CRL databases (Hassler, page 54-64). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to include a LDAP/CRL agent in the system of Kocher in order to retrieve CRL from LDAP server.

13. Claim 5 is rejected under 35 U.S.C. 103(a) as being unpatentable over Kocher (6,442,689) in view of Ng (6,411,956) and further in view of Kaliski, B; (“Kaliski”, “Privacy Enhancement for Internet Electronic Mail: Part IV: Key Certification and Related Services”, RFC 1424, Feb. 1993, pp. 1-8).

As per claim 5, Kocher and Ng teach all the claimed subject matters as discussed in claim 1, except for explicitly disclosing said plurality of CRL retrieval agents include a RFC1424/CRL retrieval agents, for periodically sending RFC1424/CRL retrieval request and receiving CRL retrieval reply. Kaliski discloses said plurality of CRL retrieval agents include a RFC1424/CRL retrieval agents, for periodically sending RFC1424/CRL retrieval request and receiving CRL retrieval reply (Kaliski, pp. 1-8). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to include a RFC1424/CRL retrieval agent in the system of Kocher in order to enhance privacy for Internet electronic mail.

Art Unit: 2172

14. Claim 9 is rejected under 35 U.S.C. 103(a) as being unpatentable over Kocher (6,442,689) in view of Ng (6,411,956) and further in view of Strellis et al. ("Strellis", 6,304,882).

As per claim 9, Kocher and Ng teach all the claimed subject matters as discussed in claim 1, except for explicitly disclosing a hub-and-spoke replication architecture is used among said central CRL database and said plurality of CR.L replication databases. Strellis discloses disclosing a hub-and-spoke replication architecture is used among said central CRL database and said plurality of CR.L replication databases (Strellis, col. 10, lines 14-21). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to use a hub-and-spoke replication architecture in the system of Kocher in order to maintain the consistency among the plurality databases.

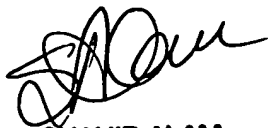
Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Chongshan Chen whose telephone number is 703-305-8319. The examiner can normally be reached on Monday - Friday (8:00 am - 4:30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, John E Breene can be reached on (703)305-9790. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703)305-3900.

December 23, 2003


SHAHID ALAM
PRIMARY EXAMINER